UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MICHELE JOHNSON and CHRISTINA SKELDON, individually, and on behalf of all others similarly situated,	)	
Plaintiffs,	)	No. 22 C 3061
v.	)	Judge Sara L. Ellis
NCR CORPORATION,	)	
Defendant.	)	

OPINION AND ORDER

Plaintiffs Michele Johnson and Christina Skeldon worked at a Wingstop restaurant in Joliet, Illinois that used a point-of-sale ("POS") system sold by Defendant NCR Corporation ("NCR"). Plaintiffs used the POS system to clock in and out of shifts, as well as to input orders. Plaintiffs filed this putative class action lawsuit alleging that NCR violated § 15(a), (b), and (d) of the Illinois Biometric Information Privacy Act ("BIPA"), 740 Ill. Comp. Stat. 14/15. NCR has moved to dismiss Plaintiffs' claims pursuant to Federal Rule of Civil Procedure 12(b)(6). Because Plaintiffs have sufficiently alleged violations of § 15(a), (b), and (d) and the Court finds that BIPA's requirements apply to third-party vendors like NCR, the Court denies NCR's motion to dismiss.

BACKGROUND[1]

NCR is a hardware, software, and service solutions vendor. It sells a biometric-enabled POS system to the restaurant industry. NCR's POS system includes POS terminals, like the NCR CX5, and cloud-based software, like NCR Aloha. NCR advertises its POS system as an

[1] The Court takes the facts in the background section from Plaintiffs' complaint and presumes them to be true for the purpose of resolving NCR's motion to dismiss. *See Phillips v. Prudential Ins. Co. of Am.*, 714 F.3d 1017, 1019–20 (7th Cir. 2013).

all-in-one solution, capable of tracking and managing workers' time and attendance as well as inputting orders. Each NCR POS terminal can be used with a biometric fingerprint scanner, which transmits the acquired biometric data to NCR's servers and to third parties that host the data. In order to access one of NCR's POS terminals, workers must scan their fingerprints. The POS system captures an image of workers' fingerprints when they enroll and then extracts unique features of the fingerprints to create unique templates associated with each worker. NCR stores the template in a database. Subsequently, each time workers provide their fingerprint, the device compares the unique features of the input fingerprints against the stored templates to verify the workers' identity. Workers' biometric data is automatically uploaded to an NCR database, where it is managed, maintained, and stored on NCR's servers. NCR also discloses the biometric data to third parties that provide it with back up storage and other IT services.

Johnson worked as a cook for Wingstop from October to November 2019 at Wingstop's Joliet, Illinois location. Skeldon worked as a cashier/night shift lead from November 2017 through June 2020 at the same Wingstop restaurant. Wingstop used NCR's POS system and required Plaintiffs to scan their fingerprints to track their time worked and otherwise access the POS terminal. NCR collected and stored Plaintiffs' biometric data in its cloud-based database. NCR did not obtain Plaintiffs' consent before disclosing or disseminating their biometric data to third parties or inform Plaintiffs in writing of the specific limited purpose or length of time for which their fingerprint data was collected, obtained, stored, used, and disseminated. Plaintiffs have not seen or learned of a publicly available biometric data retention policy or guidelines, nor have they received or signed a written release allowing NCR to collect their biometric data.

LEGAL STANDARD

A motion to dismiss under Rule 12(b)(6) challenges the sufficiency of the complaint, not its merits. Fed. R. Civ. P. 12(b)(6); *Gibson v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990). In considering a Rule 12(b)(6) motion, the Court accepts as true all well-pleaded facts in the plaintiff's complaint and draws all reasonable inferences from those facts in the plaintiff's favor. *Kubiak v. City of Chicago*, 810 F.3d 476, 480–81 (7th Cir. 2016). To survive a Rule 12(b)(6) motion, the complaint must assert a facially plausible claim and provide fair notice to the defendant of the claim's basis. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *Adams v. City of Indianapolis*, 742 F.3d 720, 728–29 (7th Cir. 2014). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678.

ANALYSIS

I. Section 15(a) Claim

Section 15(a) requires a private entity that possesses biometric information to have a "written policy made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever comes first." 740 Ill. Comp. Stat. 14/15(a). NCR argues that the Court must dismiss Plaintiffs' § 15(a) claim because they have not sufficiently pleaded that NCR possessed their biometric data, this section should not apply to third-party vendors, and, regardless, NCR has a publicly available privacy policy that satisfies § 15(a).

Because BIPA does not include a definition for "possession," *see* 740 Ill. Comp. Stat. 14/10, courts have looked to the term's "popularly understood" or "settled legal" meaning of exercising dominion or control. *Heard v. Becton, Dickinson & Co.* ("*Heard I*"), 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) (quoting *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 29)); *see also Barnett v. Apple Inc.*, 2022 IL App (1st) 220187, ¶ 42 ("[W]e apply the ordinary and popular meaning of the word "possession," as found by our supreme court and found in a dictionary, which is to have control."). NCR argues that the complaint only includes generic allegations about NCR's technology, failing to tie that technology to Plaintiffs' experiences at Wingstop. Although NCR wants greater specificity at the pleading stage, Rule 9(b) does not apply to Plaintiffs' BIPA allegations as they do not sound in fraud. *See In re Clearview AI, Inc., Consumer Priv. Litig.*, No. 21-cv-135, 2022 WL 252702, at *3 (N.D. Ill. Jan. 17, 2022) (rejecting argument that BIPA claim needed to fulfill heightened pleading standard under Rule 9(b)). Similarly, Illinois' more stringent fact-pleading standard does not apply in federal court. *See Barnett*, 2022 IL App (1st) 220187, ¶ 30–31 (comparing Illinois' fact-pleading requirements to federal courts' notice-pleading requirements). And the complaint meets Rule 8's pleading requirements, plausibly alleging that NCR exercised control over Plaintiffs' biometric data as it collected that information through the NCR POS system Plaintiffs used at the Joliet Wingstop every time they accessed the system. *See* Doc. 1-1 ¶¶ 36, 39, 55, 57. Plaintiffs need not plead more, with further factual development left for discovery.[2] *See Wilk v. Brainshark, Inc.*, No. 21-CV-4794, 2022 WL 4482842, at *5 (N.D. Ill. Sept. 27, 2022) (allegation that the defendant "obtained access to Plaintiff's uploaded video containing her biometric data; used its technology to scan Plaintiff's facial geometry from those videos and analyze those scans; and then

[2] For example, the question NCR raises in its motion of whether the Joliet Wingstop used NCR's cloud-based or non-cloud-based option is a factual one. At this stage, Plaintiffs have sufficiently alleged that Wingstop used NCR's cloud-based system.

developed reports for Plaintiff's employer" sufficed to allege dominion or control); *Heard v. Becton, Dickinson & Co.* ("*Heard II*"), 524 F. Supp. 3d 831, 840 (N.D. Ill. 2021) (plaintiff adequately pleaded possession through allegations that his biometric data was stored on the defendant's servers).

Alternatively, NCR argues that applying § 15(a) to a third-party vendor yields absurd results because, "as a back-end service provider, NCR has both no way of knowing when the 'initial purpose' for collecting data has been satisfied and no 'interaction' with Plaintiffs at all from which to base a permissible time period of retention." Doc. 19 at 12. But BIPA's text does not suggest a carveout for third-party vendors, with § 15(a) instead applying generally to any "private entity in possession of biometric identifiers or biometric information." 740 Ill. Comp. Stat. 14/15(a). And BIPA defines "private entity" broadly as "any individual, partnership, corporation, limited liability company, association, or other group, however organized." 740 Ill. Comp. Stat. 14/10. In other words, "BIPA creates a scenario where each entity's violation gives rise to a claim; a plaintiff does not incur one, indivisible injury (e.g., a broken leg or lost cargo) caused by multiple defendants, but many individual injuries at the hands of many individual defendants who violated BIPA." *Boyd v. Lazer Spot, Inc.*, No. 19 C 8173, 2022 WL 2863285, at *1 (N.D. Ill. July 20, 2022); *see also Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 787 (N.D. Ill. 2020) (third-party vendor could be held liable under BIPA "even if [the alleged] violations occurred simultaneously or through use of the same equipment" as those of the plaintiff's employer). While compliance with § 15(a)'s requirements may not be as straightforward for a third-party vendor like NCR as it would be for a direct employer, NCR has not demonstrated to the Court that BIPA exempts third-party vendors from compliance with § 15(a)'s requirements.

Finally, NCR argues that Plaintiffs' claim fails because it has a publicly available privacy policy that satisfies § 15(a). NCR's policy provides that biometric data is maintained "only for so long as it is necessary to support the overall purpose(s) for which NCR collected such information." *See* Privacy, *NCR*, https://www.ncr.com/privacy. Although the Court normally cannot consider extrinsic evidence without converting a motion to dismiss into one for summary judgment, *Jackson v. Curry*, 888 F.3d 259, 263 (7th Cir. 2018), the Court may consider "documents that are central to the complaint and are referred to in it" on a motion to dismiss, *Williamson v. Curran*, 714 F.3d 432, 436 (7th Cir. 2013). But here, Plaintiffs do not refer to the privacy policy in their complaint and so the Court does not find it appropriate to consider the policy at the pleading stage. But even were the Court to consider the policy, Plaintiffs argue that it does not comply with § 15(a) because it provides that NCR may retain biometric data as long as it deems necessary to support the purpose of collection. Taking the allegations of the complaint in the light most favorable to Plaintiffs, as the Court must at this stage, NCR's statement that it keeps biometric data "only for so long as it is necessary to support the overall purpose(s) for which NCR collected such information" does not undermine Plaintiffs' contention that NCR does not have a written retention schedule that complies with § 15(a). Thus, at this stage, the Court concludes that Plaintiffs have sufficiently pleaded a § 15(a) claim.

II. Section 15(b) Claim

Plaintiffs also claim that NCR violated § 15(b) of BIPA, which requires private entities that "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" to first obtain the individual's informed, written consent. 740 Ill. Comp. Stat. 14/15(b). Plaintiffs allege that NCR violated § 15(b) by (1) failing to inform them that NCR collected, stored, and used their biometric

information; (2) failing to inform them of the specific purpose for the collection, storage, and use, as well as the length of time NCR would retain their biometric information; and (3) failing to obtain a written release authorizing the collection or other obtainment of their biometric information.

NCR first argues that § 15(b) does not apply to it because Plaintiffs have not alleged that NCR *actively* collected, captured, or otherwise obtained their biometric information, with the complaint instead suggesting that their employer, Wingstop, collected and stored that information instead. As NCR points out, courts have recognized that possession of biometric data alone does not subject an entity to § 15(b)'s requirements. *See King v. PeopleNet Corp.*, No. 21 CV 2774, 2021 WL 5006692, at *8 (N.D. Ill. Oct. 28, 2021) ("§ 15(b) doesn't penalize mere possession of biometric information."); *Heard I*, 440 F. Supp. 3d at 965–66 ("Unlike Sections 15(a), (c), (d), and (e) of the BIPA—all of which apply to entities 'in possession of' biometric data—Section 15(b) applies to entities that 'collect, capture, purchase, receive through trade, or otherwise obtain' biometric data. Recognizing this distinction, the parties agree that mere possession of biometric data is insufficient to trigger Section 15(b)'s requirements." (citations omitted)); *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019) ("[T]here is a difference between *possessing* and *collecting* biometric information."). Thus, a number of courts have concluded that, for § 15(b) to apply, the defendant must take active steps to collect, capture, or otherwise obtain plaintiffs' biometric information. *See, e.g.*, *Jacobs v. Hanwha Techwin Am., Inc.*, No. 21 C 866, 2021 WL 3172967, at *2 (N.D. Ill. July 27, 2021) ("[P]laintiff agrees that Section 15(b) requires something more than mere possession, but is unable to articulate what that 'something more' is, if not an affirmative act of collection. . . . Following other courts in this district, this court concludes that for Section 15(b)'s requirements

to apply, an entity must, at a minimum, take an active step to collect, capture, purchase, or otherwise obtain biometric data."); *Heard I*, 440 F. Supp. 3d at 966 ("[F]or Section 15(b)'s requirements to apply, an entity must, at a minimum, take an active step to 'collect, capture, purchase, receive through trade, or otherwise obtain' biometric data." (citation omitted)). *But see Rogers v. BNSF Ry. Co.*, No. 19 C 3083, 2022 WL 4465737, at *3 (N.D. Ill. Sept. 26, 2022) (requiring an "active step" for § 15(b) claim "is a dubious proposition" because "it amounts to adding language that the statute doesn't include").

Although Plaintiffs disagree that § 15(b) requires an active step, the Court need not resolve the question here. Even assuming that Plaintiffs must plead that NCR took an active step to collect, capture, or otherwise obtain their biometric information, the complaint adequately sets forth how NCR did so. Plaintiffs allege that NCR "*actively* manages, maintains, and stores data collected from its biometric-enabled POS terminals, including biometric data, in a single, centralized location on its hosted environments and servers." Doc. 1-1 ¶ 39 (emphasis added). Plaintiffs more specifically allege that NCR's POS system captures workers' fingerprints and creates unique templates for each worker at the time of their enrollment in the database. *Id.* ¶¶ 5–6, 36, 55. According to the complaint, NCR then uses that template to create a "verifiable, user-unique audit trail that can facilitate authentication and monitoring of POS terminal access and accurate time collection." *Id.* ¶ 6, 44. In creating this audit trail, Plaintiffs maintain that NCR collected and stored their biometric data in NCR's cloud-based database on NCR's servers each time Plaintiffs accessed the POS system. *Id.* ¶¶ 7–8, 36, 57. These allegations allow for the inference that NCR took active steps to obtain Plaintiffs' biometric information. *See Smith v. Signature Sys., Inc.*, No. 2021-CV-02025, 2022 WL 595707, at *4 (N.D. Ill. Feb. 28, 2022) (complaint alleged active steps of collection by alleging that the POS system vendor scanned and

collected copies of its client's employees' fingerprints and then compared them to those stored in the database); *Heard II*, 524 F. Supp. 3d at 841 (plaintiff sufficiently alleged active steps by alleging that "when a user enrolls in the Pyxis system, the device scans the user's fingerprint, extracts the unique features of that fingerprint to create a user template, and then stores users' biometric information both on the device *and* in [defendant's] servers"); *Figueroa*, 454 F. Supp. 3d at 783–84 (allegations that the defendant stored data sufficed for § 15(b) liability because in order to store data, the defendant "necessarily first had to 'obtain' the data").

NCR nonetheless again argues that the complaint suggests that only Wingstop, Plaintiffs' employer, captured and obtained their biometric information. But in doing so, NCR attempts to rewrite the complaint to avoid its actual allegations, which allow for the reasonable inference that NCR played more than a passive role in the process. *See King*, 2021 WL 5006692, at *8 ("[I]t's reasonable to infer that PeopleNet, not its client-employers, was doing the capturing and obtaining of King's biometric information."); *cf. Jacobs*, 2021 WL 3172967, at *3 & n.2 (no active step where "a complete reading of the complaint makes clear that defendant is merely a third-party technology provider (that is, merely provided the cameras), and that the active collector and processor of the data is T.J. Maxx" and does not suggest that the third party itself "collected, obtained, or stored the biometric data"); *Bernal v. ADP, LLC*, No. 2017-CH-12364, 2019 WL 5028609, at *2 (Ill. Cir. Ct. Aug. 23, 2019) ("Plaintiff has failed to allege facts sufficient enough for the Court to properly assess Defendant's actual involvement, relative to the biometric scanning technology, beyond the fact that Defendant supplied Rockit with the technology. In order for the Court to determine whether or not § 15(b) is applicable here, Plaintiff's Complaint must include factual allegations of what Defendant's role relative to Plaintiff's biometric information is."). That suffices at this stage to plead that § 15(b) applies to

NCR. The Court leaves the question of whether Plaintiffs will actually be able to prove NCR's role in collecting and obtaining their biometric information for another day. *See Smith*, 2022 WL 595707, at *5 ("While a defendant 'may ultimately prevail' through discovery or trial on the point that it is the employer, not the defendant, that stores users' biometric information on their own systems and servers, the plaintiff 'is not required to prove the merits of his claims at the pleading stage.'" (quoting *Heard II*, 524 F. Supp. 3d at 841)).

NCR reprises another argument it made with respect to § 15(a), that § 15(b) also does not apply to outside vendors in the employment context. NCR maintains that extending § 15(b) to such third-party vendors would not further BIPA's purpose and instead would create absurd results. *See Bernal*, 2019 WL 5028609, at *1 ("While Plaintiff correctly contends that BIPA can be applied outside of an employment situation, there is nothing to suggest that BIPA was intended to apply to situations wherein the parties are without any direct relationship. . . . [T]o read BIPA as requiring that a third party provider of the biometric timeclock technology, without any direct relationship with its customers' employees, obtain written releases from said employees would be unquestionably not only inconvenient but arguably absurd."); *see also* Doc. 19-1, *Cameron v. Polar Tech Indus., Inc.*, No. 2019-CH-000013, at 33–34 (Ill. Cir. Ct. Aug. 23, 2019) (finding that § 15(b) "applies when it is an employment situation" and that "it's the employer's responsibility, not a third party['s]" to comply with the section). But *Bernal* and *Cameron* appear to be outliers, with the language on which NCR relies in *Bernal* appearing only in dicta.[3] *See Heard II*, 524 F. Supp. 3d at 843 ("The *Bernal* court's decision rested not on the

[3] NCR also cites to *Zellmer v. Facebook, Inc.*, No. 18-cv-01880, 2022 WL 976981, at *4 (N.D. Cal. Mar. 31, 2022), but *Zellmer* is distinguishable. *Zellmer* interpreted § 15(b) to require "at least a minimum level of known contact between a person and an entity that might be collecting biometric information." *Id.* Unlike in *Zellmer*, where the plaintiff was a non-Facebook user whose photograph had been uploaded by another user to the platform, *id.*, here, Plaintiffs' allegations suggest at least some level of known contact

inapplicability of Section 15(b) to third-party vendors, but on the insufficiency of the plaintiff's complaint on that count.").

More importantly, NCR cannot point to anything in BIPA's text that supports limiting § 15(b)'s reach only to employers. *See Neals v. PAR Tech. Corp.*, 419 F. Supp. 3d 1088, 1092 (N.D. Ill. 2019) ("no textual support whatsoever" exists for "the proposition that the BIPA exempts a third-party non-employer collector of biometric information when an action arises in the employment context"). True, BIPA does define "written release," used in § 15(b)(3), as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment." 740 Ill. Comp. Stat. 14/10. But this more specific definition of what constitutes a written release in the employment context does not negate the broader definition or otherwise restrict § 15(b)'s reach. *Neals*, 419 F. Supp. 3d at 1092; *see also Flores v. Motorola Sols., Inc.*, No. 1:20-cv-01128, 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021) (rejecting argument that Section 15(b)'s written consent requirement "only applies where an information collector has some relationship with the individual and has an opportunity to perform the written exchange of notice"). Nor does imposing § 15(b)'s written consent requirement on third-party vendors create absurd results. NCR "could have complied by, for example, requiring [Plaintiffs'] employer[ ], as a contractual precondition of using [NCR's] biometric timekeeping device, to agree to obtain [its] employees' written consent to [NCR] obtaining their data." *Figueroa*, 454 F. Supp. 3d at 783; *see also King*, 2021 WL 5006692, at *9 ("It's not absurd to read § 15(b) as applicable to vendors as well as employers. A waiver imposes a minor compliance cost and does not threaten BIPA's underlying purposes." (citations omitted)). Further, even if the written release requirement only applied to employers, "[s]ince

---

between NCR and workers using NCR's POS system, given the POS system's role as a timekeeping device.

the release is just one of the requirements imposed by § 15(b), the employment context of [Plaintiffs'] case doesn't excuse [NCR] from informing [Plaintiffs] that it was collecting [their] biometrics, explaining why it was using [their] information, and for how long." *King*, 2021 WL 5006692, at *9; *Heard II*, 524 F. Supp. 3d at 842 ("[E]ven if [a third-party vendor] is not required to obtain a written release from end users, it is still subject to Section 15(b)(1) and (2)."). Thus, NCR may not escape liability under § 15(b) because it does not have a direct employment relationship with Plaintiffs.

III. Section 15(d) Claim

Section 15(d) provides that private entities in possession of biometric information cannot disclose such information except under certain circumstances. 740 Ill. Comp. Stat. 14/15(d). NCR argues that the Court must dismiss Plaintiffs' § 15(d) claim because they did not sufficiently allege that NCR possessed or disclosed their biometric information. Instead, NCR maintains that Plaintiffs have merely parroted BIPA's language regarding disclosure or dissemination, which does not suffice. *See Carpenter v. McDonald's Corp.*, 580 F. Supp. 3d 512, 519 (N.D. Ill. 2022) (dismissing § 15(d) claim where "all of Plaintiff's allegations regarding disclosure, redisclosure, or dissemination are conclusions that parrot BIPA's language").

The Court has already concluded that Plaintiffs have sufficiently alleged that NCR possessed their biometric information. As for dissemination, Plaintiffs allege that "NCR discloses workers' biometric data to third-parties, which receive, store, use, access, or otherwise process the biometric data for the purpose of providing their services, including the back-up storage of data and provision of IT services." Doc. 1-1 ¶ 38. Although NCR again asks for greater specificity, Plaintiffs need not specify the who, what, when, where, and how of the dissemination to meet Rule 8's pleading requirements. *In re Clearview AI*, 2022 WL 252702, at

*3. Plaintiffs' allegations sufficiently suggest that NCR used third-party vendors and thus disseminated Plaintiffs' biometric data to them, which is all that they must do to proceed to discovery on this claim.[4] *See Naughton v. Amazon.com, Inc.*, No. 20-cv-6485, 2022 WL 19324, at *4 (N.D. Ill. Jan. 3, 2022) (plaintiff pleaded "plausible dissemination" by alleging that Amazon collected his biometric information and disclosed that information to "other Amazon entities" and "third-party biometric device and software vendor(s)"); *Heard II*, 524 F. Supp. 3d at 843 (amended complaint suggested dissemination through affirmative allegations that the employer disseminated biometric information to third-party data centers); *Wordlaw v. Enter. Leasing Co. of Chicago, LLC*, 2020 WL 7490414, at *4 (N.D. Ill. Dec. 21, 2020) (plaintiff need not include "detailed factual allegations" to support § 15(d) claim, with allegation that "Defendants implemented a timekeeping system that collected her biometrics and then shared them—without her consent—with subsidiaries, data storage vendors, and payroll service providers" enough).

CONCLUSION

For the foregoing reasons, the Court denies NCR's motion to dismiss [18].

Dated: February 6, 2023

SARA L. ELLIS
United States District Judge

[4] NCR argues that Plaintiffs concede that NCR does not disclose or disseminate their biometric data to anyone, focusing on Plaintiffs' allegation that they "have no idea whether Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data." Doc. 1-1 ¶ 49. But this is only one part of the allegation, which is predicated on the fact that Plaintiffs do not have such knowledge because NCR has failed to publish a data retention policy or otherwise disclose the purposes of the collection and use of their biometric data. *Id.* Thus, the Court does not view this allegation as precluding the § 15(d) claim, where Plaintiffs also affirmatively allege that NCR discloses their biometric data to third parties that provide IT services and back-up storage. *Id.* ¶ 38.